(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
8 juillet 2004 (08.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/057871 A2

(51) Classification internationale des brevets[7] : H04N 7/167

(21) Numéro de la demande internationale : PCT/FR2003/050181

(22) Date de dépôt international : 16 décembre 2003 (16.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02 15978 17 décembre 2002 (17.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : CANAL + TECHNOLOGIES [FR/FR]; 34 Place Raoul Dautry, F-75015 PARIS (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : DAUVOIS, Jean-Luc [FR/FR]; 19 rue Eugène Manuel, F-75116 PARIS (FR).

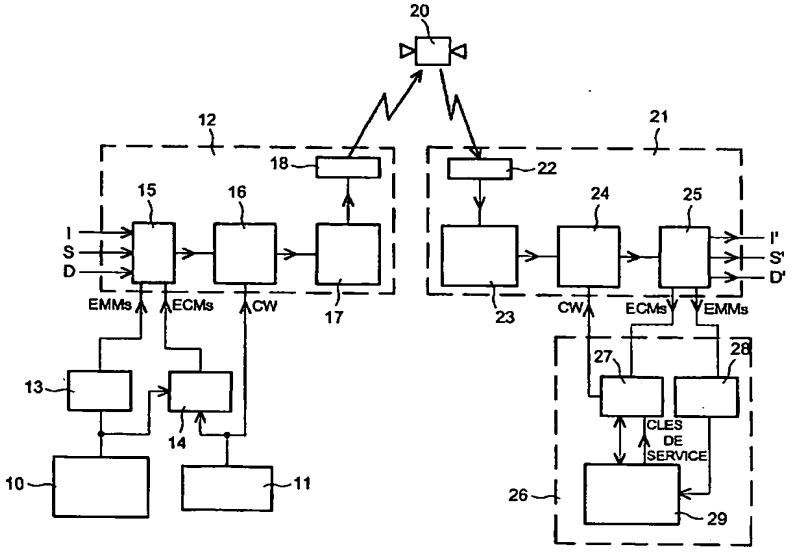
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) Title: METHOD FOR ACCESS CONTROL IN DIGITAL PAY TELEVISION

(54) Titre : PROCEDE DE CONTROLE D'ACCES EN TELEVISION NUMERIQUE PAYANTS



(57) Abstract: The invention concerns a method for controlling access, in digital pay television, to data contained in the signal received by a subscriber receiving station (21) comprising steps which consist in transmitting first right allocation control messages (ECM) enabling proposal to subscribers of an on-demand operation mode and second right allocation management messages (EMM) to a user device (26), generating in the user device an access authorization signal (CW), wherein first right allocation control messages are transmitted having a parameterable profile content enabling at least one service or one programme to be authorized during a time slot based on the profile of a specific subscriber, so as to ensure an interactivity between the content of said first messages and the content of the user's device in terms of subscription for the subscriber.

[Suite sur la page suivante]

WO 2004/057871 A2

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de contrôle d'accès, en télévision numérique payante, à des informations contenues dans un signal reçu par une station de réception abonné (21) comprenant des étapes d'émission de premiers messages de contrôle d'allocation de droits (ECM) permettant de proposer aux abonnés un mode de fonctionnement à la demande et de seconds messages de gestion d'allocation de droits (EMM) vers un dispositif utilisateur (26), de génération dans le dispositif utilisateur (26) d'un signal d'autorisation d'accès (CW), dans lequel on émet des premiers messages de contrôle d'allocation de droits ayant un contenu de profil paramétrable permettant d'autoriser au moins un service ou un programme pendant une certaine fenêtre de temps en fonction du profil d'un abonné déterminé, de maniere à réaliser une certaine interactivité entre le contenu de ces premiers messages et le contenu du dispositif utilisateur en termes d'abonnement pour l'abonné.

PROCEDE DE CONTROLE D'ACCES EN TELEVISION NUMERIQUE PAYANTE

DESCRIPTION

DOMAINE TECHNIQUE

La présente invention concerne un procédé de contrôle d'accès dans le domaine de la télévision numérique payante.

ETAT DE LA TECHNIQUE ANTERIEURE

Les techniques utilisées en télévision payante sont basées sur deux mécanismes indépendants : d'une part sur un brouillage/cryptage des signaux vidéo et/ou audio, d'autre part sur une fonction d'allocation de droits commerciaux qui sont transmis comme des messages sécurisés à un boîtier de débrouillage (avec accès de contrôle). Le cryptage peut être appliqué aisément sur un flot de bits numérique. Tous les bits peuvent être cryptés en utilisant par exemple un chiffrage par blocs. Le brouillage est utilisé pour des émissions analogiques. En utilisant un tel brouillage le format du signal est changé, les signaux de synchronisation sont supprimés et transmis séparément sous une forme cryptée. Le signal audio peut être converti en un signal numérique puis crypté. Le signal audio numérique crypté peut être inséré dans le signal vidéo.

Les données transmises sont brouillées ou cryptées en utilisant un mot de contrôle (CW) ou une clé. Le mot de contrôle ou la clé changent après une

courte période. Pour envoyer de nouvelles clés à la station de réception abonné, des messages ECM de contrôle d'allocation de droits ("Entitlement Control Messages") et des messages EMM de gestion d'allocation de droits ("Entitlement Management Messages") sont utilisés.

Ces deux messages ECM et EMM peuvent être envoyés au travers de la station de réception abonné à une carte à puce.

Les messages ECM contiennent des informations qui permettent à la station de réception abonné de débrouiller les signaux vidéo et/ou audio. Les données de débrouillage sont retournées à celle-ci sous une forme qui ne permet le débrouillage que si l'utilisateur est autorisé à accéder au programme de télévision en cours. Lorsqu'un utilisateur est représenté par une carte à puce, l'autorisation d'accès est indiquée par des données d'allocation de droits ("entitlement data") mémorisées dans la carte.

Les messages EMM contiennent des informations qui permettent de mettre à jour les données d'allocation de droits de l'utilisateur, par exemple en modifiant les données mémorisées dans la carte à puce.

Les messages ECM et EMM ont un champ de signature numérique qui assure l'intégrité du message (par exemple un code de Hash). Ceci évite aux utilisateurs de pouvoir modifier le contenu de leurs messages.

Un message ECM est émis avec le signal brouillé transmis. Il comprend trois champs. Le premier

champ contient les paramètres d'accès. Ces paramètres définissent les conditions dans lesquelles l'accès à un programme de télévision est permis. Ce champ rend, par exemple, possibles une appréciation parentale (un code PIN additionnel est alors requis par le décodeur) et une occultation géographique (un film peut n'être disponible dans tous les pays européen). Le second champ contient un mot de contrôle sous forme cryptée. Le dernier champ contient un contrôle d'intégrité des données.

Un message EMM contient usuellement quatre champs. Chaque message EMM débute avec un champ adresse pour sélectionner un (des) récepteur(s). Il y a deux modes d'adressage, l'un pour une station individuelle et l'autre pour un groupe de telles stations. Le second champ contient une allocation de droits pour un utilisateur donné. Le troisième champ contient les clés de service sous forme cryptée. Le dernier champ contient un contrôle d'intégrité des données. Les messages EMM peuvent aussi être utilisés pour envoyer une commande au décodeur. L'émission de messages EMM est généralement le résultat d'une requête explicite de l'utilisateur au fournisseur de service. Ces messages sont en général individuels. Les messages EMM ne sont pas émis de façon synchrone avec le service de télévision auquel ils s'appliquent. Ils sont transmis à l'avance afin de permettre l'accès à un programme donné d'un utilisateur autorisé. N'importe quel réseau peut être utilisé pour transmettre ces messages EMM au récepteur : modem, courrier ou radiodiffusion.

Pour augmenter la probabilité qu'un message EMM a été reçu par l'utilisateur, pour renouveler une souscription par exemple, celui-ci est envoyé plusieurs fois. Les messages EMM sont ainsi organisés cycliquement selon une période donnée pour l'émission. La durée d'une telle période est le paramètre principal pour déterminer le temps maximum à attendre pour obtenir une allocation de droit pour un utilisateur qui a coupé sa station de réception pendant une longue durée.

Un article de l'art connu, intitulé "Functional model of a conditional access system" (8301 EBU Review Technical, 1995, n°266), décrit un modèle fonctionnel de système d'accès conditionnel pour une utilisation en télévision numérique. Un tel système d'accès conditionnel comprend une combinaison de brouillage et de cryptage pour éviter toute réception non autorisée, le brouillage permettant de rendre les images, le son et les données non intelligibles, le cryptage protégeant les clés secrètes qui ont été transmises avec le signal brouillé afin de permettre au débrouilleur de fonctionner. Après le débrouillage, tout défaut sur les images ou le son doit être imperceptible, c'est-à-dire que ce système d'accès conditionnel doit être transparent.

La génération, la transmission et l'utilisation de messages de gestion d'allocation de droits (EMMS) par le système d'autorisation abonné sont illustrés sur la figure unique.

Ce système d'autorisation d'abonné 10 (SAS ou "Subscriber Autorisation System) ainsi qu'un

générateur 11 de mot de contrôle (CW) sont reliés à une station d'émission d'opérateur 12, chacun via un circuit de cryptage 13 et 14.

Cette station d'émission d'opérateur 12 reçoit des signaux image I, son S et données D qui transitent successivement au travers d'un multiplexeur 15, d'un brouilleur 16, d'un modulateur 17 et d'un émetteur 18.

A la réception des signaux émis par ledit émetteur 18 et transmis, par exemple, par l'intermédiaire d'un satellite 20, une station de réception abonné 21, qui comprend successivement un récepteur 22, un démodulateur 23, un débrouilleur 24, un démultiplexeur 25, délivre des signaux image I', son S', et données D'.

Un sous-système d'accès conditionnel, par exemple une carte à puce 26, qui comprend deux circuits de décryptage 27 et 28 et un processeur de sécurité 29 (clés secrètes) est relié à cette station de réception abonné 21.

Le débrouillage nécessite de posséder un débrouilleur, un circuit de décryptage et une clé service courante. Le décryptage nécessite l'utilisation de messages de gestion d'allocation de droits (EMM) pour le programme courant, qui utilise usuellement des clés secrètes mémorisées dans la carte à puce 26.

Dans le domaine de la télévision numérique un mode de consommation à la demande peut être proposé aux abonnés. Ce mode de consommation permet de visualiser un service, par exemple une séance de cinéma, en mode abonnement avec une réservation de

séance ou un fonctionnement de type "impulsive pay per view/pay per time" (paiement pour voir/paiement pour une certaine durée impulsifs).

Mais un tel mode de consommation ne permet pas de faire des offres promotionnelles directement chez un abonné, ni même d'autoriser un service de façon ciblée, par exemple voir un programme donné pendant une certaine fenêtre de temps, en fonction du profil d'un abonné déterminé, de manière à cibler une certaine tranche de population d'abonnés, sans devoir envoyer des messages de gestion d'allocation de droits (EMM) de validation puis de dévalidation.

L'invention a pour objet de résoudre un tel problème en prévoyant un nouveau mode de consommation permettant d'autoriser un service de façon ciblée et à distance en fonction d'un profil d'abonnée déterminé, sans entrainer de forte contrainte sur la station d'émission d'opérateur.

EXPOSÉ DE L'INVENTION

La présente invention propose donc un procédé de contrôle d'accès, en télévision numérique payante, à des informations contenues dans un signal reçu par une station de réception abonné comprenant des étapes :

- d'émission de deux types de messages via cette station de réception abonné vers un dispositif utilisateur, des premiers messages de contrôle d'allocation de droits contenant des informations pour permettre à cette station de réception abonné de décoder le signal et pour proposer aux abonnés un mode de fonctionnement à la demande, des seconds messages de

gestion d'allocation de droits contenant des informations pour permettre la mise à jour des données d'allocation de droits de l'utilisateur,

- de génération dans le dispositif utilisateur d'un signal d'autorisation d'accès pour permettre le décodage dudit signal par la station de réception abonné si l'utilisateur est autorisé à accéder aux informations contenues dans celle-ci,

caractérisé en ce qu'on émet des premiers messages de contrôle d'allocation de droits ayant un contenu de profil paramétrable permettant d'autoriser au moins un service ou un programme pendant une certaine fenêtre de temps en fonction du profil d'un abonné déterminé, de manière à réaliser une certaine interactivité entre le contenu de ces premiers messages et le contenu du dispositif utilisateur en termes d'abonnement pour l'abonné.

Le procédé de l'invention permet avantageusement :

- de faire des offres promotionnelles, avec réduction du nombre de messages de gestion d'allocation de droits (EMM) transmis,

- de réaliser un "profiling" (tenir compte du profil des abonnés) aisément,

- de lutter contre le piratage système.

Ce procédé permet, en effet, de lutter contre un certain type de piratage système, qui consiste pour un abonné donné, à un instant déterminé, de demander une offre d'abonnement maximale puis après réception du message de gestion d'allocation de droits

(EMM) de validation, de demander l'abonnement de base tout en éliminant les messages de gestion d'allocation de droits (EMM) suivants, comprenant notamment le message EMM de révocation.

BRÈVE DESCRIPTION DES DESSINS

La figure unique illustre un système d'émission-réception de signaux de télévision numérique de l'art connu.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

Dans le procédé de l'invention, qui fonctionne dans un système tel qu'illustré sur la figure, les messages de contrôle d'allocation de droits ECM ont un contenu de profil paramétrable, ce qui permet de réaliser une certaine interactivité entre le contenu de tels messages ECM et le contenu de la carte à puce, en termes d'abonnement pour l'abonné.

Il est ainsi possible, pour des abonnés, qui bénéficient d'une première offre O1 et d'une seconde offre O2, de pouvoir bénéficier d'une troisième offre O3 sous le contrôle des messages ECM, pendant la durée d'un film par exemple. Si l'on veut alors ne plus faire une telle offre en promotion on retire la condition des messages ECM.

Une telle caractéristique permet une visualisation de certains services en fonction du profil des abonnés, sans avoir à envoyer, au préalable, un grand nombre de messages de gestion d'allocation de droits EMM.

Elle permet, également, de faire bénéficier d'un prix réduit les abonnés ayant un certain profil. Par exemple un abonné ayant payé des droits pour des programmes P1 et P2 et une offre commerciale O1 peut payer un programme à acheter 2 jetons, alors que les autres utilisateurs ont à payer 4 jetons.

Une telle caractéristique permet, également, de lutter contre le piratage système. Selon le procédé de l'invention, pour chaque service ou chaque programme est attribuée une offre temporaire journalière. Lorsqu'un abonné demande à avoir accès à un programme, par exemple une séance de cinéma, plutôt que lui donner accès à une offre permanente, on lui donne accès à une offre temporaire.

Ainsi si dans un laps de temps court, par exemple la même journée, cet abonné demande une offre d'abonnement maximale puis change d'avis et, pour ne pas payer, demande à bénéficier de l'abonnement de base, usuellement un message de gestion d'allocation de droits EMM de révocation lui est envoyé. Si celui-ci, alors, utilise un "blocker" de ces messages EMM, pour éliminer ceux-ci, il peut alors continuer à avoir accès au service demandé, ou au programme demandé, gratuitement pendant, par exemple, deux mois.

Par contre avec le procédé de l'invention, puisque l'offre est temporaire, le lendemain, par exemple, l'abonné n'a plus accès au service, ou au programme, même s'il a utilisé un "blocker EMM". Pour les abonnés ayant demandé et confirmé leur offre maximale, il est toutefois nécessaire d'envoyer un

message EMM de révocation avec l'offre permanente de ce service, ou de ce programme.

Exemple de mise en œuvre du procédé de l'invention

. avec des contenus conditionnels

De tels contenus conditionnels des messages EMM permettent de travailler en utilisant des fonctions ET, OU, SI, SINON et NON, sur les champs Bitmap que représentent l'adressage géographique et/ou l'adressage abonnement. Ils permettent, également, de réaliser un fonctionnement conditionnel entre des numéros de programmes, par exemple un achat de tel programme si tel autre programme a déjà été acheté.

Un tel mode de fonctionnement conditionnel se présente sous la forme d'une séquence, par exemple :

SI (offre 01) ET (offre 02) ET (NON offre 03)

- Achat programme P1 en mode "Impulsive pay per view" proposé à 50 jetons.

SINON

- Achat programme P1 en mode "Impulsive pay per view" proposé à 70 jetons.

FINSI

.avec des bitmaps conditionnels

On peut utiliser des mécanismes conditionnels pour offrir à un abonné des possibilités d'achats ou de visualisation additionnels, par exemple :

SI (((offre 01) ET ((offre 03) OU (offre 04))) OU (offre 02)

visualisation possible d'un programme
FINSI.

.avec lutte contre un piratage système

On peut utiliser des mécanismes conditionnels pour lutter contre le type de piratage décrit ci-dessus, par exemple :

- au jour to

SI ((offre temporaire 05) OU (offre permanente 01))
- visualisation possible d'un programme
FINSI

- au jour to + 1

SI ((offre temporaire 06) OU (offre permanente 01))
- visualisation possible de ce programme
FINSI.

REVENDICATIONS

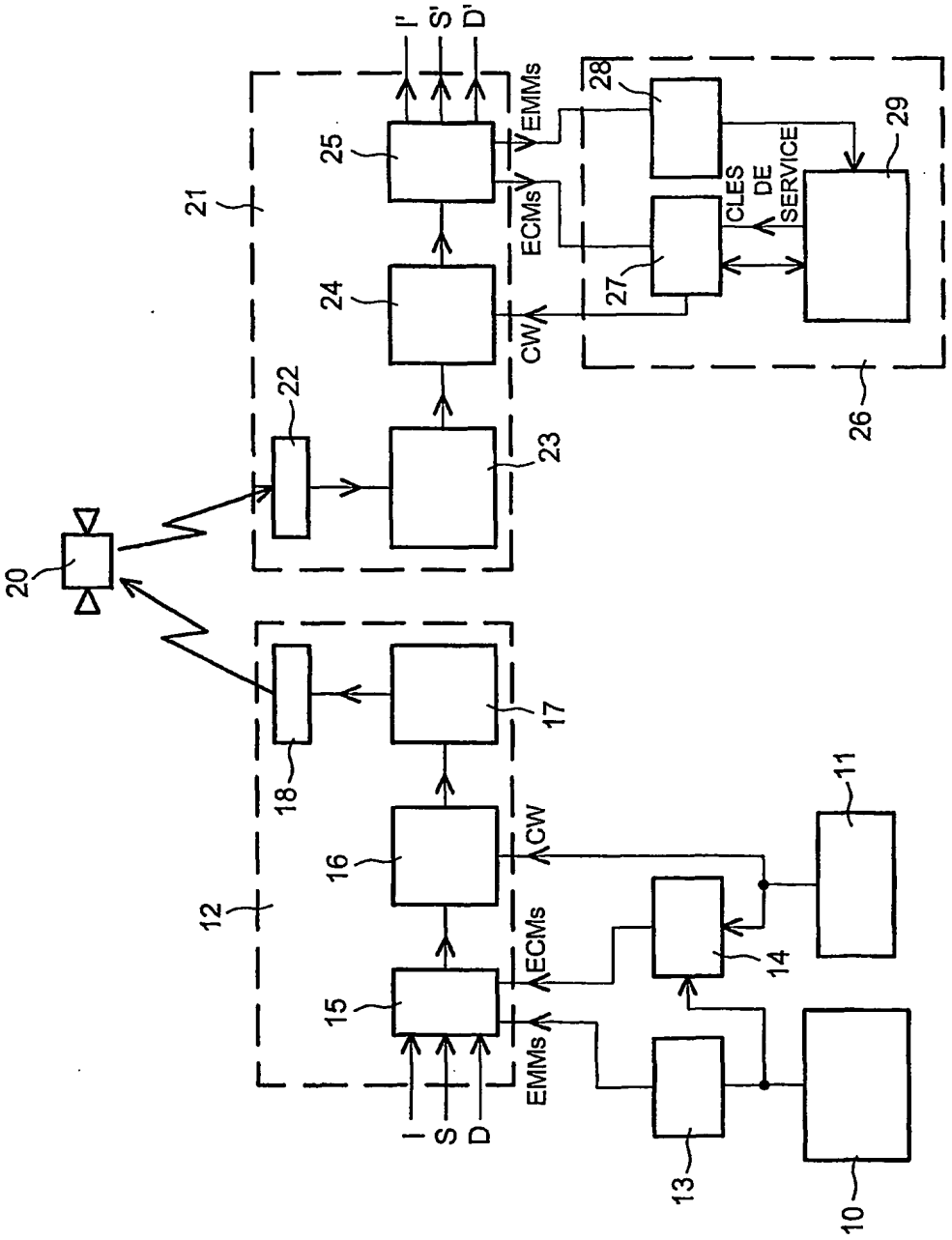
1. Procédé de contrôle d'accès, en télévision numérique payante, à des informations contenues dans un signal reçu par une station de réception abonné (21) comprenant des étapes :

- d'émission de deux types de messages via cette station de réception abonné vers un dispositif utilisateur (26), des premiers messages de contrôle d'allocation de droits (ECM) contenant des informations pour permettre à cette station de réception abonné de décoder le signal et pour proposer aux abonnés un mode de fonctionnement à la demande, des seconds messages de gestion d'allocation de droits (EMM) contenant des informations pour permettre la mise à jour des données d'allocation de droits de l'utilisateur,

- de génération dans le dispositif utilisateur (26) d'un signal d'autorisation d'accès (CW) pour permettre le décodage dudit signal par la station de réception abonné (21) si l'utilisateur est autorisé à accéder aux informations contenues dans celle-ci,

caractérisé en ce qu'on émet des premiers messages de contrôle d'allocation de droits (ECM) ayant un contenu de profil paramétrable permettant d'autoriser au moins un service ou un programme pendant une certaine fenêtre de temps en fonction du profil d'un abonné déterminé, de manière à réaliser une certaine interactivité entre le contenu de ces premiers messages (ECM) et le contenu du dispositif utilisateur en termes d'abonnement pour l'abonné.

2. Procédé selon la revendication 1, dans lequel le dispositif utilisateur est une carte à puce.


I' S' D'
EMMs
ECMs
CW
CLES
DE
SERVICE
I S D
EMMs
ECMs
CW
20
21
22
23
24
25
26
27
28
29
12
15
16
17
18
10
11
13
14